1. Introduction

Protecting and ensuring the continuity of the critical infrastructure and key resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. CIKR includes systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on national security, national economic security, public health or safety, or any combination of those matters. Terrorist attacks on our CIKR, as well as other manmade or natural disasters, could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the affected CIKR and physical location of the incident. Direct and indirect impacts could result in large-scale human casualties, property destruction, economic disruption, and mission failure, and also significantly damage national morale and public confidence. Terrorist attacks using components of the Nation's CIKR as weapons of mass destruction (WMD)[1] could have even more devastating physical, psychological, and economic consequences.

Protecting the Nation's CIKR is essential to making America safer, more secure, and more resilient in the context of terrorist attacks and other natural and manmade hazards. **Protection** includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the National Infrastructure Protection Plan (NIPP), this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other manmade or natural disaster (see figure 1-1). Protection can include a wide range of activities such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating active or passive countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, and business continuity planning, among others. The NIPP (June 2006; revised January 2009) and its complementary Sector-Specific Plans (SSPs) (May 2007; to be reissued in 2010) provide a

Figure 1-1: Protection

[1] (1)Any explosive, incendiary, or poison gas (i) bomb, (ii) grenade, (iii) rocket having a propellant charge of more than 4 ounces, (iv) missile having an explosive or incendiary charge of more than one-quarter ounce, (v) mine, or (vi) similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. 2332a).

consistent, unifying structure for integrating both existing and future CIKR protection efforts. The NIPP also provides the core coordinating processes and mechanisms that enable all levels of government and private sector partners to work together to implement CIKR protection in an effective and efficient manner.

The NIPP was developed through extensive coordination with partners at all levels of government and the private sector. NIPP processes are designed to be adapted and tailored to individual sector and partner requirements, including State, local, or regional issues. Participation in the implementation of the NIPP provides government and the private sector with the opportunity to use collective expertise and experience to more clearly define issues and solutions, and to ensure that existing CIKR protection approaches and efforts, including business continuity and resiliency planning, are recognized.

Since the NIPP and the SSPs were first released, the processes and programs outlined in those documents have continued to evolve and mature. This update to the NIPP reflects many advances, including:

- The issuance of the SSPs, which followed the release of the NIPP;
- Establishment of Critical Manufacturing as the 18th CIKR sector and the designation of Education as a subsector of Government Facilities;
- Expansion of the sector partnership model to include the geographically focused Regional Consortium Coordinating Council (RCCC);
- CIKR mission integration within State and local fusion centers;
- Evolution of the National Asset Database to the Infrastructure Information Collection System and the Infrastructure Data Warehouse;
- Developments in the programs, approaches, and tools used to implement the NIPP risk management framework;
- Updates on risk methodologies, information-sharing mechanisms, and other CIKR protection programs;
- Inclusion of outcome-focused performance measurement and reporting processes;
- Description of additional Homeland Security Presidential Directives, national strategies, and legislation;
- Release of the Chemical Facility Anti-Terrorism Standards (CFATS), establishing a regulatory framework for those industries that involve the production, use, and storage of high-risk chemicals;
- Discussion of expanded CIKR protection-related education, training, outreach, and exercise programs;
- Evolution from the National Response Plan to the National Response Framework (NRF); and
- Inclusion of further information on research and development (R&D) and modeling, simulation, and analysis processes and initiatives.

Additionally, the revised NIPP integrates the concepts of resiliency and protection, and broadens the focus of NIPP-related programs and activities to an all-hazards environment.

1.1 Purpose

The NIPP provides the framework for the unprecedented cooperation that is needed to develop, implement, and maintain a coordinated national effort to bring together government at all levels, the private sector, nongovernmental organizations, and international partners. The NIPP depends on supporting SSPs for full implementation of this framework within and across CIKR sectors. SSPs are developed by the Federal Sector-Specific Agencies (SSAs) designated in Homeland Security Presidential Directive 7 (HSPD-7) in close collaboration with sector partners.

Together, the NIPP and SSPs provide the mechanisms for: identifying critical assets, systems, and networks, and their associated functions; understanding threats to CIKR; identifying and assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are applied where they offer the greatest mitigation of risk; and enhancing information-sharing mechanisms and protection and resiliency within and across CIKR sectors. The NIPP and SSPs will evolve along with changes to the Nation's CIKR and the risk environment, as well as evolving strategies and technologies for protecting against and responding to threats and incidents. Implementation of the NIPP and the SSPs occurs at all levels through actions taken by: Federal agencies; State, regional, local, tribal, and territorial governments and organizations; and individual CIKR owners and operators.

1.2 Scope

The NIPP considers a full range of physical, cyber, and human risk elements within and across sectors. In accordance with the policy direction established in HSPD-7, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, and the National Strategy to Secure Cyberspace, the NIPP includes a special focus on the unique and potentially catastrophic impact of terrorist attacks. At the same time, the NIPP builds on and is structured to be consistent with and supportive of the Nation's all-hazards approach to homeland security preparedness and domestic incident management. Many of the benefits of enhanced CIKR protection are most sustainable when protective programs and resiliency strategies are designed to address all hazards.

The NIPP addresses ongoing and future activities within each of the CIKR sectors identified in HSPD-7 and across the sectors regionally, nationally, and within individual States or communities. It defines processes and mechanisms used to prioritize protection of U.S. CIKR (including territories and territorial seas) and to address the interconnected global networks upon which the Nation's CIKR depend. The processes outlined in the NIPP and the SSPs recognize that protective measures do not end at a facility's fence or at a national border, and are often a component of a larger business continuity approach. Also considered are the implications of cross-border infrastructures, international vulnerabilities, and cross-sector dependencies and interdependencies.

1.3 Applicability

The NIPP is applicable to a wide array of public and private sector CIKR partners in different ways. The framework generally is applicable to all partners with CIKR protection responsibilities and includes explicit roles and responsibilities for the Federal Government, including CIKR under the control of independent regulatory agencies, and the legislative, executive, and judicial branches. Federal departments and agencies with specific responsibilities for CIKR protection are required to take actions that are consistent with HSPD-7. The NIPP also provides an organizing structure, guidelines, and recommended activities for other partners to help ensure consistent implementation of the national framework and the most effective use of resources. State,[2] local,[3] tribal, and territorial government partners are required to establish CIKR protection programs that are consistent with the National Preparedness Guidelines and as a condition of eligibility for certain Federal grant programs.

Owners and operators are encouraged to participate in the NIPP partnership and to initiate measures to augment existing plans for risk management, resiliency, business continuity, and incident management and emergency response in line with the NIPP framework.

1.3.1 Goal

The overarching goal of the NIPP is to:

> ***Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of our Nation's CIKR, and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.***

Achieving this goal requires understanding and sharing information about terrorist threats and other hazards, building partnerships, implementing a long-term risk management program, and maximizing the efficient use of resources. Measuring progress toward achieving the NIPP goal requires that CIKR partners strive toward:

- Coordinated CIKR risk management plans and programs that are in place to address known and potential threats and hazards;
- Structures and processes that are flexible and adaptable both to incorporate operational lessons learned and best practices, and also to quickly reflect a changing threat or incident environment;
- Processes in place to identify and address dependencies and interdependencies to allow for more timely and effective implementation of short-term protective actions and more rapid response and recovery; and
- Access to robust information-sharing networks that include relevant intelligence and threat analysis, and real-time incident reporting.

[2] Consistent with the definition of "State" in the Homeland Security Act of 2002, all references to States within the NIPP are applicable to the territories and include by reference any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States (Homeland Security Act).

[3] A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or, in Alaska, a Native village or Alaska Regional Native Corporation; and a rural community, unincorporated town or village, or other public entity (Homeland Security Act).

1.3.2 The Value Proposition

The public-private partnership called for in the NIPP provides the foundation for effective CIKR protection. Prevention, response, mitigation, and recovery efforts are most efficient and effective when there is the full participation of government and industry partners; the mission suffers (e.g., full benefits are not realized) without the robust participation of a wide array of CIKR partners.

The success of the NIPP partnership depends on articulating the benefits to government and the private sector partners. Industry capabilities that add value to the government include:

- Understanding of CIKR assets, systems, networks, and facilities, and other capabilities through industry ownership and management of a vast majority of CIKR in most sectors;
- Ability to take action to reduce risk and to respond to and recover from incidents;
- Ability to innovate and to provide products, services, and technologies to quickly focus on mission needs; and
- Robust relationships that are useful for sharing and protecting sensitive information regarding threats, vulnerabilities, countermeasures, and best practices.

Although articulating the value proposition to the government typically is easier to achieve, it is often more difficult to articulate the direct benefits of participation for the private sector. In assessing the value proposition for the private sector, there is a clear national interest in ensuring the collective protection and resiliency of the Nation's CIKR. More specific benefits that have been realized during the first few years of the partnership include:

- Participation in both a policy development and risk analysis and management framework that helps focus both corporate and government planning and resource investment;
- Greater information sharing regarding specific threats and hazards enabled by the issuance of security clearances to private sector partners;
- Leveraged application of preparedness guidelines and self-assessment tools within and across sectors so that risks can be managed more effectively and efficiently from the corporate level down to the individual facility level;
- Targeted application of limited resources to the highest risk issues, to include Federal grant funding where appropriate;
- Coordination and planning across multiple agencies for those assets and facilities that are considered to be at the greatest risk;
- Joint R&D and modeling, simulation, and analysis programs;
- Participation in national-level and cross-sector training and exercise programs, as well as the National Incident Management System;
- Access and input into cross-sector interdependency analyses;
- Established informal networks among private sector partners and between the private sector and the various Federal agencies that can be used for all-hazards planning and response; and
- Identification of potential improvements in regulations.

Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale CIKR protection through activities such as:

- Providing owners and operators with timely, accurate, and useful analysis and information on threats to CIKR;
- Ensuring that industry is engaged as early as possible in the development of policies and initiatives related to NIPP implementation;
- Articulating to corporate leaders, through the use of public platforms and private communications, both the business and national security benefits of investing in security measures that exceed their business case;
- Creating an environment that encourages and supports incentives and recognition for companies to voluntarily adopt widely accepted security practices;
- Working with industry to develop and clearly prioritize key missions and enable the protection and/or restoration of related CIKR;
- Providing support for R&D initiatives that is needed to enhance future CIKR protection efforts;
- Providing the resources to enable cross-sector interdependency studies; exercises, symposiums, training sessions, and computer modeling; and otherwise support business continuity planning; and
- Enabling time-sensitive information sharing and restoration and recovery support to priority CIKR facilities and services during emerging threat and incident management situations.

The above examples illustrate some of the ways in which the government can partner with the private sector to add value to industry's ability to assess risk and refine its own business continuity and security plans, as well as to contribute to the security and sustained economic vitality of the Nation.

1.4 Threats to the Nation's CIKR

Presidential guidance and national strategies issued in the aftermath of the September 11, 2001, attacks focused initial CIKR protection efforts on addressing the terrorist threat environment. These new challenges required approaches that focused on intelligence-driven analyses, information sharing, and unprecedented partnerships between the government and the private sector at all levels. The Nation's CIKR owners and operators have decades of experience planning for and responding to natural disasters, industrial accidents, and the deliberate acts of malicious individuals in order to maintain business continuity. However, such plans and preparedness efforts must continue to adapt to a dynamic threat environment and to address vulnerabilities and gaps in CIKR protection in an all-hazards context.

1.4.1 The Vulnerability of the U.S. Infrastructure to 21st Century Threats and Hazards

America is an open, technologically sophisticated, highly interconnected, and complex Nation with a wide array of infrastructure that spans important aspects of the U.S. Government, economy, and society. The vast majority of the CIKR-related assets, systems, and networks are owned and operated by the private sector. However, in sectors such as Water and Government Facilities, the majority of owners and operators are governmental or quasi-governmental entities. The great diversity and redundancy of the Nation's CIKR provide for significant physical and economic resilience in the face of terrorist attacks, natural disasters, or other emergencies, and contribute to the strength of the Nation's economy. However, this vast and diverse aggregation of highly interconnected assets, systems, and networks may also present an attractive array of targets to domestic and international terrorists and magnify greatly the potential for cascading failure in the wake of catastrophic natural or manmade disasters. Improvements in protection and resilience that focus on elements of CIKR that are deemed to be nationally critical can make it more difficult for terrorists to launch destructive attacks, as well as lessen the impact of any attack or other disaster that does occur and provide greater resiliency in response and recovery.

1.4.2 The Nature of the Terrorist Adversary

The number and high profile of international and domestic terrorist attacks and disrupted plots during the last two decades underscore the determination and persistence of terrorist organizations. Terrorists have proven to be relentless, patient, opportunistic, and flexible, learning from experience and modifying tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. Analysis of terrorist goals and motivations points to domestic and international CIKR as potentially prime targets for terrorist attacks. As security measures around more predictable targets increase, terrorists are likely to shift their focus to less protected targets. Enhancing countermeasures to address any one terrorist tactic or target may increase the likelihood that terrorists will shift to another, which underscores the necessity for a balanced, comparative approach that focuses on managing risk commensurately across all sectors and scenarios of concern.

Terrorist organizations have shown an understanding of the potential consequences of carefully planned attacks on economic, transportation, and symbolic targets, both within the United States and abroad. Future terrorist attacks against CIKR located inside the United States and those located abroad could seriously threaten national security, result in mass casualties, weaken the economy, and damage public morale and confidence.

The NIPP considers a broad range of terrorist objectives, intentions, and capabilities to assess the threat to various components of the Nation's CIKR. Terrorists may contemplate attacks against the Nation's CIKR to achieve direct or indirect effects, or to exploit the infrastructure to cause catastrophic loss of life or economic disruptions.

The NIPP outlines the ways in which the Department of Homeland Security (DHS) and its partners use threat analysis to inform comprehensive risk assessments and risk-mitigation activities. The risk management framework discussed in chapter 3 strikes a balance between ways to mitigate specific threats and general threats. It ensures that the range of risk scenarios considered is broad enough to avoid a "failure of imagination," yet provides a process to enable risk assessment sufficient for the purpose of formulating action plans and programs to enhance resiliency, reduce vulnerability, deter threats, and mitigate potential consequences.

1.4.3 All-Hazards and CIKR Protection

In addition to addressing CIKR protection related to terrorist threats, the NIPP also describes activities relevant to CIKR protection and preparedness in an all-hazards context. The direct impact, disruption, and cascading effects of natural disasters (e.g., Hurricanes Katrina and Rita, the Northridge earthquake, the 2008 Mississippi River floods) and manmade incidents (e.g., the Minneapolis I-35 bridge collapse or the Exxon Valdez oil spill) are documented and underscore the vulnerabilities and interdependencies of the Nation's CIKR.

Many owners and operators, government emergency managers, and first-responders have developed strategies, plans, policies, and procedures to prepare for, mitigate, respond to, and recover from a variety of natural and manmade incidents. The NIPP framework supports these efforts and, additionally, provides an augmented focus on the protection of America's CIKR against terrorist attacks. In fact, the day-to-day public-private coordination structures, information-sharing networks, and risk management frameworks used to implement NIPP steady-state CIKR protection efforts continue to function and provide the CIKR protection dimension for incident management under the National Response Framework (NRF). Likewise, the mitigation and business continuity practices employed to protect against natural hazards and other non-terrorist attacks should support and augment the goals of the NIPP. The NIPP, and the public and private sector partnership that it represents, work in conjunction with other plans and initiatives to provide a strong foundation for preparedness in an all-hazards context.

1.5 Special Considerations

CIKR protection planning involves special consideration for unique cyber elements that support CIKR operations and complex international relationships—two areas of recent focus and attention.

1.5.1 The Cyber Dimension

- The U.S. economy and national security depend greatly and increasingly on the global cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CIKR.
- A spectrum of malicious actors routinely conducts attacks against the cyber infrastructure using cyber attack tools. Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating effect.
- Cybersecurity includes preventing damage to, unauthorized use of, or exploitation of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Cybersecurity also includes restoring electronic information and communications systems in the event of a terrorist attack or natural disaster.
- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's vulnerability to cyber threats if cybersecurity is not addressed and integrated appropriately.

Cyber infrastructure includes electronic information and communication systems, and the information contained in these systems. Computer systems, control systems such as Supervisory Control and Data Acquisition (SCADA) systems, and networks such as the Internet are all part of cyber infrastructure.

Information and communications systems are composed of hardware and software that process, store, and communicate data of all types. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.

Information Technology (IT) critical functions are sets of processes that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (e.g., R&D, manufacturing, distribution, upgrades, and maintenance) involved in transforming supply inputs into IT products and services.

- The interconnected and interdependent nature of the Nation's CIKR makes it problematic to address the protection of physical and cyber assets independently.
- The NIPP addresses reducing cyber risk and enhancing cybersecurity in two ways: (1) as a cross-sector cyber element that involves DHS, SSAs and Government Coordinating Councils (GCCs), and private sector owners and operators; and (2) as a major component of the Information Technology Sector's responsibility in partnership with the Communications Sector.

1.5.2 International CIKR Protection

- The NIPP addresses international CIKR protection, including interdependencies and vulnerabilities based on threats (and associated consequences) that originate outside the country or pass through it.
- The Federal Government and the private sector work with foreign governments and international/multinational organizations to enhance the confidentiality, integrity, and availability of cyber infrastructure and products.
- Protection of assets, systems, and networks that operate across or near the borders with Canada and Mexico, or rely on other international aspects to enable critical functionality, requires coordination with and planning and/or sharing resources among neighboring governments at all levels, as well as private sector CIKR owners and operators.
- The Federal Government and private sector corporations have a significant number of facilities located outside the United States that may be considered CIKR.

- Special consideration may be required when CIKR is extensively integrated into an international or global market (e.g., financial services, agriculture, energy, transportation, telecommunications, or information technology) or when a sector relies on inputs that are not within the control of U.S. entities.
- Special consideration is required when government facilities and functions are directly affected by foreign-owned and -operated commercial facilities.
- The Federal Government, working in close coordination and cooperation with the private sector, launched the Critical Foreign Dependencies Initiative in 2007 to identify assets and systems located outside the United States, which, if disrupted or destroyed, would critically affect public health and safety, the economy, or national security. The resulting strategic compendium guides engagement with foreign countries in the CIKR protection mission area.

1.6 Achieving the Goal of the NIPP

Achieving the NIPP goal of building a safer, more secure, and more resilient America requires actions that address the following principal objectives:

- Understanding and sharing information about terrorist threats and other hazards;
- Building partnerships to share information and implement CIKR protection and resiliency programs;
- Implementing a long-term risk management program that includes:
  - Hardening, distributing, diversifying, and otherwise ensuring the resiliency of CIKR against known threats and hazards, as well as other potential contingencies;
  - Developing processes to interdict human threats to prevent potential attacks;
  - Planning for rapid response to CIKR disruptions to limit the impact on public health and safety, the economy, and government functions; and
  - Planning for rapid CIKR recovery for those events that are not preventable; and
- Maximizing the efficient use of resources for CIKR protection.

This section provides a summary of the actions needed to address these objectives. More detailed discussions of these actions are included in the chapters that follow.

1.6.1 Understanding and Sharing Information

One of the essential elements needed to achieve the Nation's CIKR protection goals is to ensure the availability and flow of accurate, timely, and relevant information and/or intelligence about terrorist threats and other hazards, information analysis, and incident reporting. This includes:

- Establishing effective information-sharing processes and protocols among CIKR partners;
- Providing intelligence and information to SSAs and other CIKR sector partners as permitted by law;
- Analyzing, warehousing, and sharing risk assessment data in a secure manner that is consistent with relevant legal requirements and information protection responsibilities;
- Providing protocols for real-time threat and incident reporting, alert, and warning; and
- Providing protocols for the protection of sensitive information.

Chapter 3 details the risk and threat analysis processes and products aimed at better understanding and characterizing terrorist threats. Chapter 4 describes the NIPP network approach to information sharing and the process for protecting sensitive CIKR-related information.

1.6.2 Building Partnerships

Building partnerships represents the foundation of the national CIKR protection effort. These partnerships provide a framework to:

- Exchange ideas, approaches, and best practices;
- Facilitate security planning and resource allocation;
- Establish effective coordinating structures among partners;
- Enhance coordination with the international community; and
- Build public awareness.

Chapters 2 and 4 describe partners' roles and responsibilities related to CIKR protection, as well as specific mechanisms for the governance, coordination, and information sharing necessary to enable effective partnerships.

1.6.3 Implementing a CIKR Risk Management Program

The risk management program detailed in the NIPP includes processes to:

- Establish a risk management framework to guide CIKR protection and resiliency programs and activities;
- Take appropriate risk management actions to enhance CIKR protection and resiliency based on all-hazards risk assessments;
- Conduct and update risk assessments, as appropriate, at the asset, system, network, sector, cross-sector, regional, national, and international levels;
- Develop and deploy new technologies to enable more effective and efficient CIKR protection; and
- Provide a system for measurement and improvement of CIKR protection, including:
  - Establishing performance metrics to track the effectiveness of protection programs and resiliency strategies; and
  - Updating the NIPP and SSPs as required.

The NIPP also specifies the processes, initiatives, and milestones necessary to implement an effective long-term CIKR risk management program. Chapter 3 provides details regarding the NIPP risk management framework and the measurement and analysis processes that support its continuous improvement; chapter 6 addresses issues that are important for sustaining and improving CIKR protection over the long term.

1.6.4 Maximizing Efficient Use of Resources for CIKR Protection

Maximizing the efficient use of resources for CIKR protection includes a coordinated and integrated annual process for program implementation that:

- Supports prioritization of programs and activities within and across sectors considering sector needs and requirements;
- Informs the annual Federal process regarding planning, programming, and budgeting for national-level CIKR protection;
- Helps align Federal resources with the CIKR protection mission and supports the tracking and accountability of public funds;
- Considers State, local, tribal, and territorial government and private sector issues related to planning, programming, and budgeting;
- Draws on expertise across organizational and national boundaries;
- Shares expertise and speeds implementation of best practices;
- Recognizes the need to build a business case to support further private sector CIKR protection investments; and
- Identifies potential incentives for preparedness and security-related activities where they do not naturally exist in the marketplace.

Chapter 5 explains how a coordinated national approach to the CIKR protection mission supports the efficient application of resources. Efficient use of resources enables the continuous improvement of the technology, databases, data systems, and other approaches used to protect CIKR and manage risk. These processes are detailed in chapter 6. Chapter 7 describes the annual processes that reflect coordination with SSAs and other partners regarding resource prioritization and allocation. Also discussed are processes to target grants and other funding authorities to maximize and focus the use of resources to support national and sector priorities.

More information about the NIPP is available on the Internet at: www.dhs.gov/nipp or by contacting DHS at: nipp@dhs.gov